hcpc health & care professions council

Council, 25 May 2017

Information Governance Report 2016

Introduction

1.1 The Information Governance (IG) function within the Secretariat Department is responsible for the HCPC's ongoing compliance with the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR) and the Data Protection Act 1998 (DPA). The Department also manages the HCPC's relationship with the Information Commissioner's Office (ICO), the information rights body.

1.2 At its meeting in March 2017 the Council agreed that it would receive annual IG reports in future. This report provides an overview of IG activity in 2016.

Information requests

2.1 As a public body, the HCPC is covered by the FOIA. As such we are required to publish certain information about our activities proactively, as well as respond to specific requests for information from members of the public.

2.2 In 2016, the HCPC received 524 information requests. This is a slight decrease of 4% from 2015 when the total was 547.

2.3 Requests are roughly split between registration statistics or specific FTP case information, with occasional requests for HR or financial information.

2.4 In April 2016, a new, part-time role of Information Governance Officer was created within the Secretariat department. One of the main responsibilities of the postholder is to assist in the management of the volume of requests received, with the dedicated resource being better able to respond to increases or complex requests that take more time.

2.5 The table below shows the monthly totals for requests for information over the past 3 years.

Information requests
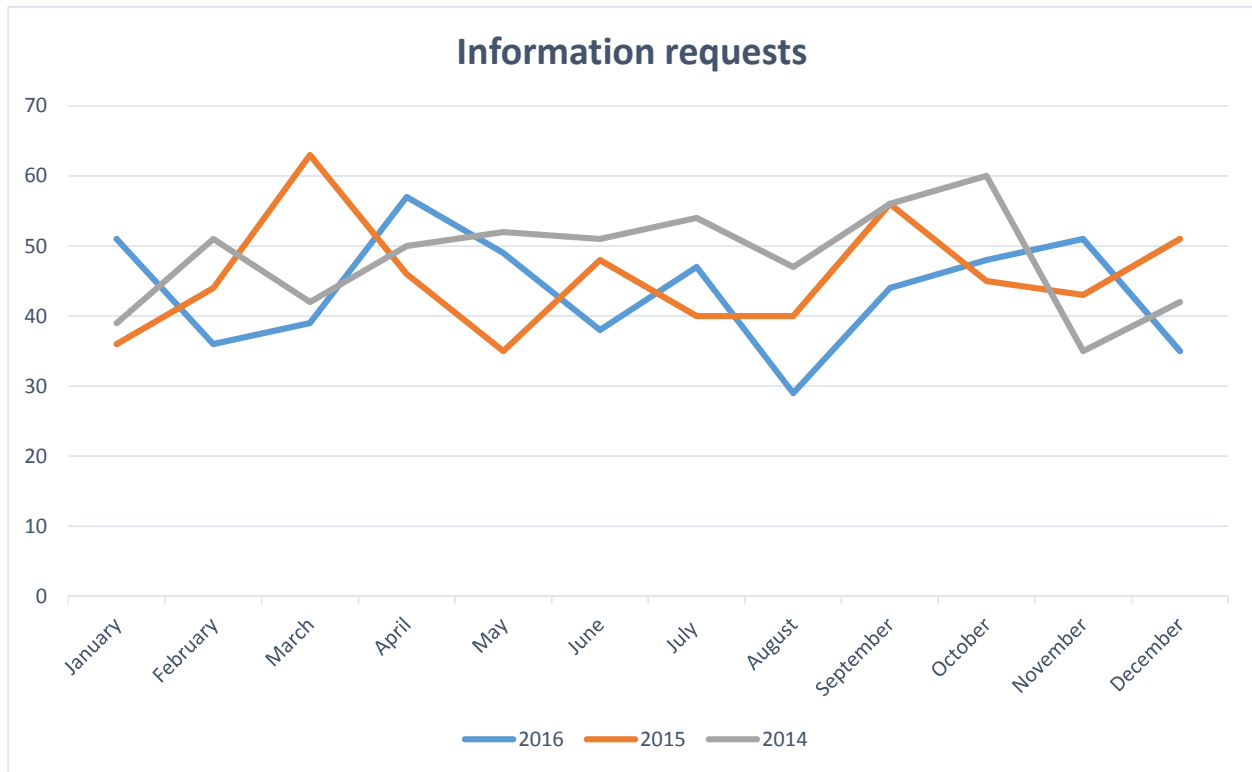
2.6   No discernible trends are apparent in the distribution of requests.

2.7   A FOI policy was published on the HCPC website in January 2017. The policy
       aims to assist members of the public to understand what information is
       available to them and the process of making an FOI request.
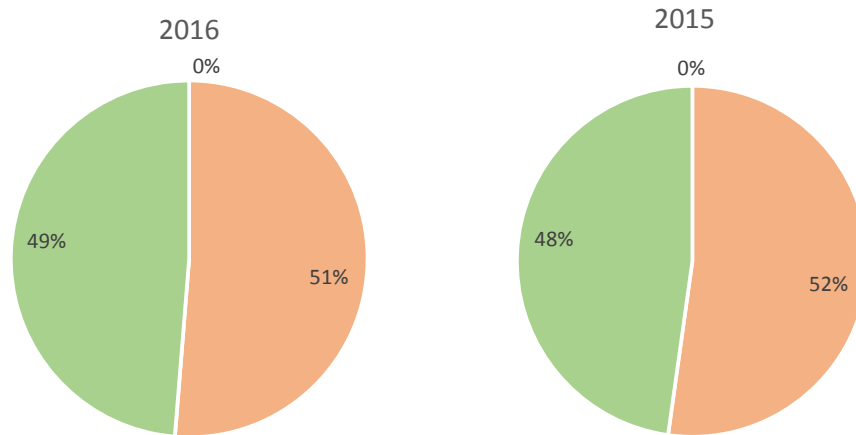
Information Incident Management

3.1   An information incident is where personal data has been unintentionally
       disclosed, altered or lost. Since February 2015, all incidents, regardless of
       how minor they may initially appear, are reported centrally and risk assessed.

3.2   The HCPC encourages an open reporting culture, with an emphasis on
       analysis and learning in order to engineer-out any weaknesses in our
       processes, much like the feedback and complaints function

3.3   In 2016, the HCPC recorded 78 information incidents. This is a decrease of
       31% on the total for 2015 which was 113.

3.4   Incidents are risk scored based on potential harm to the data subject. These
       are then classified as red, amber or green ratings in terms of severity.

2.5   In 2016, 49% of incidents were rated green, 51% were amber. The charts below show classifications in 2016 and 2015. There were no incidents rated red.

3.6   The HCPC's information incident management compliance is reviewed by the ISO 27001 audit. The HCPC recently achieved recertification to this standard.

3.7   No incidents have been reported to the ICO in 2016 or 2015. Two were reported in 2014 but these did not meet the ICO's threshold for enforcement and were closed with no further action.

Information Governance

4.1   The General Data Protection Regulations (GDPR) were approved by the EU Parliament in April 2016 and will come into force from 25 May 2018. The GDPR will replace the DPA in the UK.

4.2   The primary objectives of the GDPR are to give EU citizens control of their personal data, simplify the regulatory environment for businesses by unifying data protection practices within the EU and update current regulations to take into account technology changes.

4.3   The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR. The UK was a promoter of the reform and will be required to adhere to its standard of data protection if it wishes to trade with EU member states in future.

4.4   The ICO has begun to provide guidance to organisations on transitioning to the GDPR. However this is at an early stage, and detailed guidance on many of the key changes is yet to be published.

4.5   In April 2017, EMT considered a gap analysis paper and a review of compliance has begun. This will be led by the Information Governance function during 2017-2018 and reported to Council as appropriate.

4.6   The majority of the requirements of the GDPR are already required by the DPA. Therefore, the HCPC's good standard of compliance with DPA will make the transition to GDPR easier.

4.7   While on the whole, our approach to compliance will remain valid, there are new elements and enhancements required by GDPR that will require the HCPC to build on its current compliance practice.

4.8   In April 2017, the HCPC attended the Health Regulators Information Security Special Interest Group, the focus of which was GDPR and the regulators shared plans for compliance preparation. A further meeting on GDPR is planned for September, at this point it is expected there will be more detailed guidance issued on key aspects.

Decision

The Council is requested to discuss the report; no decision is required.

Appendices

None.

Date of paper

4 May 2017.